TWO COMBINATORIAL GEOMETRIC PROBLEMS INVOLVING MODULAR HYPERBOLAS

MIZAN R. KHAN, RICHARD MAGNER, STEVEN SENGER, AND ARNE WINTERHOF

Abstract. For integers a and $n \geq 1$ with $\gcd(a, n) = 1$ let $\overline{\mathcal{H}}_{a,n}$ be the set of least residues of a modular hyperbola

$$\overline{\mathcal{H}}_{a,n} = \{(x, y) \in \mathbb{Z}^2 : xy \equiv a \pmod{n}, 1 \leq x, y \leq n-1\}.$$

In this paper we prove two combinatorial geometric results about $\overline{\mathcal{H}}_{a,p^m}$, where p^m is a prime power. Our first result shows that the number of ordinary lines spanned by $\overline{\mathcal{H}}_{1,p^m}$ is at least

$$(p-1)p^{m-1}\left(\frac{p^{m-1}(p-2)}{2} + c(p^m)\right),$$

where $c(p^m) = 3/4 + o(1)$ if $m \geq 2$ and $p > 2$, $c(2^m) = 1/2$ if m is sufficiently large, $c(p^m) = 6/13$ if $m \geq 2$, p^m is small and $p^m \neq 8$, and $c(p) = 0$. For $m = 1$ we have equality.

The second result gives a partial answer to a question of Shparlinski [8] on the cardinality of

$$\mathcal{F}_{a,n} = \{\sqrt{x^2 + y^2} : (x, y) \in \overline{\mathcal{H}}_{a,n}\}.$$

1. Ordinary lines in $\overline{\mathcal{H}}_{p^m}$

Let $\mathbb{Z}_n^*$ be the group of invertible elements modulo n and let $\mathcal{H}_{a,n}$ denote the *modular hyperbola* $xy \equiv a \pmod{n}$ where $x, y, a \in \mathbb{Z}$, with $\gcd(a, n) = 1$. (We insert the condition that a and n are relatively prime to ensure that $\mathcal{H}_{a,n} \subseteq \mathbb{Z}_n^* \times \mathbb{Z}_n^*$.) Following [8] we define $\overline{\mathcal{H}}_{a,n} = \mathcal{H}_{a,n} \cap [1, n-1]$, that is,

$$\overline{\mathcal{H}}_{a,n} = \{(x, y) \in \mathbb{Z}^2 : xy \equiv a \pmod{n}, 1 \leq x, y \leq n-1\}.$$

In the special case of $\overline{\mathcal{H}}_{1,n}$ we will simply drop the 1 and write $\overline{\mathcal{H}}_n$.

Let S be a finite set of points in the Euclidean space. A line that passes through exactly two distinct points of S is said to be an *ordinary*

Date: April 26, 2013.

1991 *Mathematics Subject Classification.* 11A05, 11A07, 52C30.

line spanned by S. The notion of an ordinary point arose in the context of the famous *Sylvester-Gallai* theorem in combinatorial geometry.

Theorem 1 (Sylvester-Gallai)**.** *Let P be a set of points in the plane, not all on a plane. Then there is an ordinary line spanned by P.*

We refer the reader to [6] and the references therein for an exposition of the history of this theorem and subsequent developments. We now give an application of the Sylvester-Gallai theorem to modular hyperbolas.

Lemma 2. *The only moduli for which the modular hyperbolas $\overline{\mathcal{H}}_n$ do* not *span an ordinary line are $n = 2, 8, 12$ and 24.*

Proof. We assume that $n \neq 2, 3, 4, 6$. For $n = 2$ the modular hyperbola consists of only one point. In the case of $n = 3, 4$ or 6 the modular hyperbola consists of only two points and so for these 3 cases we have precisely one ordinary line.

The points $(1, 1)$ and $(n - 1, n - 1)$ are two distinct points of $\overline{\mathcal{H}}_n$, and consequently $\overline{\mathcal{H}}_n$ spans the line $y = x$. We now observe that the number of solutions of the congruence $z^2 \equiv 1 \pmod{n}$ equals $\varphi(n)$ precisely when $n = 2, 3, 4, 6, 8, 12$ and 24. For all other values of n there exists $z \in \mathbb{Z}_n^*$ such that $z^2 \not\equiv 1 \pmod{n}$. Such a z gives a point in $\overline{\mathcal{H}}_n$ that does not lie on $y = x$. We now invoke the Sylvester-Gallai theorem to conclude our proof. $\square$

For prime moduli it is easy to determine the precise number of ordinary lines.

Lemma 3. *Let p be a prime. Then the set $\overline{\mathcal{H}}_{a,p}$ spans $(p-1)(p-2)/2$ ordinary lines.*

Proof. We show that any line connecting 2 different points of $\overline{\mathcal{H}}_{a,p}$ is ordinary. Let $(x_1, y_1), (x_2, y_2)$ be two distinct points in $\overline{\mathcal{H}}_{a,p}$, that is in particular $x_1 \neq x_2$ and $y_1 \neq y_2$, and let $y = kx + d$ be the line in $\mathbb{R}^2$ passing through these two points. Then x_1, x_2 are distinct roots modulo p of the quadratic polynomial $kx^2 + dx - a$. By Lagrange's theorem $kx^2 + dx - a$ has no more than 2 roots modulo p. Hence, no other point of $\overline{\mathcal{H}}_{a,p}$ lies on $y = kx + d$ and the $\binom{p-1}{2}$ lines are all ordinary. $\square$

For the rest of this section we focus on the case $a = 1$ and notice that for prime powers p^m with $m \geq 2$ (and $p^m \neq 4$) such a result no longer holds as $\overline{\mathcal{H}}_{p^m}$ spans lines that are not ordinary. In particular we have the following example.

Lemma 4. *Let p be a prime and let $m \in \mathbb{Z}$ with $m \geq 2$ and $p^m > 8$. Then $\overline{\mathcal{H}}_{p^m}$ spans a line with $\left(p^{\lfloor m/2 \rfloor} - 1\right)$ points.*

Proof. We include the hypothesis $p^m > 8$ to ensure that $\left(p^{\lfloor m/2 \rfloor} - 1\right) \geq 2$. Consider the line

$$L : x + y = p^m + 2.$$

We show that the cardinality of the intersection

$$\#\left(\overline{\mathcal{H}}_{p^m} \cap L\right) = p^{\lfloor m/2 \rfloor} - 1.$$

The lattice points on the line L that lie inside the first quadrant are of the form $(k, p^m + 2 - k)$ with $k = 1, 2, \ldots, p^m, p^m + 1$. Now if $(k, p^m + 2 - k) \in \overline{\mathcal{H}}_{p^m}$, then we have that

$$k(2 - k) \equiv 1 \pmod{p^m},$$

which we rewrite as

$$(k - 1)^2 \equiv 0 \pmod{p^m}.$$

Therefore,

$$k - 1 = lp^{\lceil m/2 \rceil}$$

with $l = 1, 2, \ldots, \left(p^{\lfloor m/2 \rfloor} - 1\right)$. □

However, a slight modification of the proof of Lemma 1 allows us to give a lower bound for the number of ordinary lines spanned by $\overline{\mathcal{H}}_{p^m}$.

For small p^m we will need to invoke the following weaker version of the Dirac-Motzkin conjecture proved by Csima and Sawyer [4].

Theorem 5. *Suppose P is a finite set of n points in the plane, not all on a line and $n \neq 7$. Then P spans at least $6n/13$ ordinary lines.*

The Dirac-Motzkin conjecture states that the lower bound for the number of ordinary lines is $n/2$ for sufficiently large n. Green and Tao [6, Theorem 2.2] in a 2013 preprint on arxiv have confirmed a more precise version of this conjecture which implies the following result.

Theorem 6. *Suppose P is a finite set of n points in the plane, not all on a line and n is sufficiently large. Then P spans at least $n(3/4+o(1))$ ordinary lines if n is odd and at least $n/2$ ordinary lines if n is even.*

We now state our first main result.

Theorem 7. *Let p^m be a prime power and N the number of ordinary lines that $\overline{\mathcal{H}}_{p^m}$ spans. Then*

$$N \geq p^{m-1}(p-1)\left(\frac{p^{m-1}(p-2)}{2} + c(p^m)\right),$$

where $c(p^m) = 3/4 + o(1)$ if $m \geq 2$ and $p > 2$, $c(2^m) = 1/2$ if m is sufficiently large, $c(p^m) = 6/13$ if $m \geq 2$, p^m is small and $p^m \neq 8$, and $c(p) = 0$. For $m = 1$ we have equality.

We partition $\overline{\mathcal{H}}_{p^m}$ into the disjoint sets $C_i, i = 1, 2, \ldots, p-1$, where

$$C_i = \{(x, y) \in \overline{\mathcal{H}}_{p^m} : x \equiv i \pmod{p}\}.$$

Our proof of Theorem 7 rests on the following lemmas.

Lemma 8. *Let $m \geq 2$ be an integer and let L be a line*

$$L : ax + by + c = 0 \text{ with } \gcd(a, b, c) = 1.$$

We have the following:

(i) *Let (x_1, y_1) and (x_2, y_2) be two distinct points on $L \cap \overline{\mathcal{H}}_{p^m}$. If $x_1 \equiv x_2 \pmod{p}$, then*

$$2ax_1 \equiv -c \pmod{p};$$

and if $y_1 \equiv y_2 \pmod{p}$, then

$$2by_1 \equiv -c \pmod{p}.$$

(ii) *If $\gcd(ab, p) = p$, then $\#(L \cap \overline{\mathcal{H}}_{p^m}) \leq 1$. In other words, if L is spanned by $\overline{\mathcal{H}}_{p^m}$, then $\gcd(ab, p) = 1$.*

(iii) *If $\#(L \cap \overline{\mathcal{H}}_{p^m}) \geq 3$, then for some i,*

$$\left(L \cap \overline{\mathcal{H}}_{p^m}\right) \subseteq C_i.$$

Furthermore, $c^2 - 4ab \equiv 0 \pmod{p}$.

Proof. Throughout the proof we will use $f(x)$ to denote the polynomial $ax^2 + cx + b$.

(i) We prove the case when $x_1 \equiv x_2 \pmod{p}$. Now,

$$a(x+h)^2 + c(x+h) + b = (ax^2 + cx + b) + (2ax + c)h + ah^2.$$

Setting $x = x_1$ and $h = x_2 - x_1$ we obtain

$$ax_2^2 + cx_2 + b = (ax_1^2 + cx_1 + b) + (2ax_1 + c)(x_2 - x_1) + a(x_2 - x_1)^2.$$

Since $f(x_1) \equiv f(x_2) \equiv 0 \pmod{p^m}$, we get

$$(2ax_1 + c + a(x_2 - x_1))(x_2 - x_1) \equiv 0 \pmod{p^m}.$$

Since $x_1 \equiv x_2 \pmod{p}$, but $x_1 \not\equiv x_2 \pmod{p^m}$, we infer that

$$2ax_1 + c + a(x_2 - x_1) \equiv 0 \pmod{p^l}$$

for some $l, 0 < l < m$, and conclude that

$$2ax_1 + c \equiv 0 \pmod{p}.$$

(ii) Without loss of generality we can assume that $p|a$. Let (x_1, y_1) and (x_2, y_2) be two distinct points in $L \cap \overline{\mathcal{H}}_{p^m}$. Therefore

$$f(x_1) \equiv f(x_2) \equiv 0 \pmod{p^m}.$$

Since $p|a$, $f(x)$ reduces modulo p to the linear polynomial $cx+b$. Since x_1 and x_2 are both zeros of the congruence $cx + b \equiv 0 \pmod{p}$, we conclude that $x_1 \equiv x_2 \pmod{p}$. Now by part 1 we conclude that $-c \equiv 2ax_1 \equiv 0 \pmod{p}$. Since $p|a$, we have that $p|c$ and consequently $p|b$, which gives the contradiction $\gcd(a, b, c) \neq 1$. Therefore if $p|a$, then

$$\#(L \cap \overline{\mathcal{H}}_{p^m}) < 2.$$

(iii) Suppose

$$L \cap \overline{\mathcal{H}}_{p^m} = \{(x_1, y_2), (x_2, y_2), \ldots, (x_n, y_n)\},$$

with $n \geq 3$. By part 2 we have that $\gcd(ab, p) = 1$. We now show that

$$x_1 \equiv x_2 \equiv x_3 \equiv \ldots \equiv x_n \pmod{p}.$$

The integers $x_1, x_2, \ldots, x_n$ are zeros of $f(x)$ modulo p^m. Since p is a prime and since $f(x)$ has at least one zero modulo p, we can factor $f(x)$ as

$$f(x) = a(x - r)(x - s) \pmod{p}.$$

Clearly $x_i \equiv r \pmod p$ or $x_i \equiv s \pmod p$ for $i = 1, \ldots, n$. We now prove that $r \equiv s \pmod p$ by showing that $f'(r) \equiv 0 \pmod p$. Without loss of generality we can assume that $x_1 \equiv x_2 \equiv r \pmod p$. Now on invoking part 1 we obtain

$$2ar + c \equiv 0 \ (\mathrm{mod}\ p), \text{ that is, } f'(r) \equiv 0 \ (\mathrm{mod}\ p).$$

Thus $(L \cap \overline{\mathcal{H}}_{p^m}) \subseteq C_i$ where $i = -c \cdot (2a)^{-1} \mod p$. We note that since $f(x)$ has only one root modulo p, the discriminant $c^2 - 4ab$ is divisible by p. □

Lemma 9. *For any $i, i = 1, 2, \ldots, p-1$, not all of the points of C_i lie on a line.*

Proof. We argue by contradiction. Suppose there exists a line L such that $C_i = L \cap \overline{\mathcal{H}}_{p^m}$. Let $j = i^{-1} \mod p$. By choosing the points on C_i whose x-coordinates are i and $i + p$ respectively, we infer that the slope of the line L is an integer. The line $y = x$ is a line of symmetry of $\overline{\mathcal{H}}_{p^m}$. If we reflect the line L along this line, then we get a line L' such that $L' \cap \overline{\mathcal{H}}_{p^m} = C_j$. By the same argument as before we get that the slope of L' is an integer. Furthermore slope$(L) \cdot$ slope$(L') = 1$ and consequently slope$(L) = \pm 1$.

Suppose slope$(L) = -1$. The point $(i, j + kp) \in (L \cap \overline{\mathcal{H}}_{p^m})$ for some $k, 1 \le k < p^{m-1}$. We now once again invoke the fact that the line $x = y$ is a line of symmetry of $\overline{\mathcal{H}}_{p^m}$. The reflection of L along the line $x = y$ is L itself. In particular $(j + kp, i) \in (L \cap \overline{\mathcal{H}}_{p^m})$. Therefore $i \equiv j \pmod p$, that is, $i^2 \equiv 1 \pmod p$, from which we obtain that $i = 1$ or $i = p - 1$, that is, $C_i = C_1$ or $C_i = C_{p-1}$. However, neither the points of C_1 nor the points of C_{p-1} can lie on a line of slope -1. In the case of C_1, the point $(1, 1) \in C_1$ and the line of slope -1 passing $(1, 1)$ contains no other points of C_1. A similar observation with the point $(p^m - 1, p^m - 1)$ takes care of C_{p-1}.

So the last case to consider is slope$(L) = 1$. Since the slope is 1, the only way that L can contain all of the points of C_i is if

$$C_i = \{(i + kp, j + kp) \,:\, k = 0, 1, \ldots, p^m - 1\}.$$

Since $1 \le i, j \le p - 1$, $i \cdot j < p^m$. Therefore, for $i \cdot j \equiv 1 \pmod{p^m}$, we must have that $i \cdot j = 1$, that is $(i, j) = (1, 1)$. However the intersection

of the line $x = y$ with $\overline{\mathcal{H}}_{p^m}$ consists solely of two points:

$$(1, 1) \text{ and } (p^m - 1, p^m - 1).$$

□

Proof of Theorem 7. If $(x_1, y_1) \in C_i$ and $(x_2, y_2) \in C_j$ with $i \neq j$, then Lemma 8 shows that the line through the points (x_1, y_1) and (x_2, y_2) is ordinary. There are $(p-2)(p-1)p^{2(m-1)}/2$ possible such pairs of points. Furthermore, since the points of C_i do not all lie on a line, by Theorem 5 or Theorem 6, respectively, each C_i gives rise to at least $c(m)p^{m-1}$ ordinary lines. From these observations we conclude that

$$N \geq p^{m-1}(p-1)\left(\frac{p^{m-1}(p-2)}{2} + c(p^m)\right).$$

□

An upper bound for the number of points of $\overline{\mathcal{H}}_{p^m}$ on a line. In Lemma 4 we showed that

$$\#\left(L \cap C_1\right) = p^{\lfloor m/2 \rfloor} - 1,$$

where L is the line

$$L : x + y = p^m + 2 \text{ and } C_i = \{(x, y) \in \overline{\mathcal{H}}_{p^m} \,:\, x \equiv i \pmod{p}\}.$$

We now prove the following result that indicates that this is an extreme example.

Proposition 10. *Let $m \geq 2$ be an integer and let*

$$L : ax + by + c = 0,$$

be a line that is spanned by $\overline{\mathcal{H}}_{p^m}$. Then

$$\#\left(L \cap \overline{\mathcal{H}}_{p^m}\right) \leq p^{m/2} + p^{(m-1)/2} - p^{1/2} - 1, \quad p > 2.$$

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be a polynomial in x with integer coefficients, α be an integer such that $\gcd(\alpha, p) = 1$, and

$$e_q(x) = \exp\left(\frac{2\pi\sqrt{-1}\,x}{q}\right).$$

The exponential sum $S(f, q)$ is defined via

$$S(f, q) = \sum_{x=0}^{q-1} e_q(f(x)),$$

which we rewrite as the sum

$$S(f,q)=\sum_{\alpha=0}^{p-1} S_\alpha(f,q)$$

where $S_\alpha(f,q)$ is defined via

$$S_\alpha(f,q)=\sum_{x=0}^{q/p-1} e_q(f(\alpha+px)).$$

These exponential sums were studied by Cochrane and Zheng in [3]. We will need the following results which are part of Theorem 2.1 in [3].

Theorem 11. *Let $q=p^m$ with p an odd prime and $m\geq 2$. Furthermore we assume that*

$$\gcd\left(na_n,(n-1)a_{n-1},\dots,2a_2,a_1,p\right)=1.$$

(i) *If α is not a zero of the congruence $f'(x)\equiv 0 \pmod p$, then*

$$S_\alpha(f,q)=0.$$

(ii) *If α is a zero of the congruence $f'(x)\equiv 0 \pmod p$ of multiplicity 1, then*

$$|S_\alpha(f,q)|\leq\sqrt{q}. \tag{1}$$

Proof of Proposition 10. We prove our result by expressing the quantity $\#\left(L\cap\overline{\mathcal{H}}_q\right)$ by an exponential sum and then applying inequality (1). Without loss of generality we can assume that L is not ordinary and $\gcd(a,b,c)=1$. By Lemma 8 we have that $\gcd(ab,p)=1$ with $c^2\equiv 4ab \pmod p$. Furthermore any points on $L\cap\overline{\mathcal{H}}_{p^m}$ must lie in

$$C_\alpha=\{\alpha+pk\,:\,k=0,\dots,q-1\},$$

where $\alpha=-c\cdot(2a)^{-1} \mod p$.

Let $f(x)=ax^2+cx+b$. For $x\in\mathbb{Z}$,

$$\frac{1}{q}\sum_{k=0}^{q-1} e_q(kf(x))=\begin{cases}1, & f(x)\equiv 0 \pmod q\\ 0, & f(x)\not\equiv 0 \pmod q.\end{cases}$$

Consequently,

$$q\cdot\#\left(\overline{\mathcal{H}}_q\cap L\right)\leq\sum_{x\in C_\alpha}\sum_{k=0}^{q-1} e_q(kf(x)).$$

By interchanging the sums we obtain that

$$\sum_{x\in C_\alpha}\sum_{k=0}^{q-1} e_q(kf(x)) = \sum_{k=0}^{q-1} S_\alpha(kf,q).$$

Now

$$\sum_{k=0}^{q-1} S_\alpha(kf,q) = \sum_{t=0}^{m-1}\sum_{k=1,\gcd(k,q)=p^t}^{q-1} S_\alpha(kf,q) + p^{m-1}. \tag{2}$$

We now invoke the following property of the exponential sum S_α: if $k = p^t l$, with $1 \le t \le m-1$ and $\gcd(l,p) = 1$, then

$$S_\alpha(kf,q) = \begin{cases} p^t S_\alpha(lf, q/p^t), & t \le m-2 \\ p^{m-1} e_p(lf(\alpha)), & t = m-1. \end{cases}$$

We obtain that the RHS of (2) equals

$$\sum_{t=0}^{m-2}\sum_{k=1,\gcd(k,p)=1}^{q/p^t-1} p^t S_\alpha(kf,q/p^t) + p^{m-1}\sum_{l=1}^{p-1} e_p(lf(\alpha)) + p^{m-1}.$$

The last two terms cancel each other and we obtain

$$\sum_{k=0}^{q-1} S_\alpha(kf,q) = \sum_{t=0}^{m-2}\sum_{k=1,\gcd(k,p)=1}^{q/p^t-1} p^t S_\alpha(kf,q/p^t).$$

By repeatedly invoking the inequality (1) to the RHS we obtain that

$$\sum_{k=0}^{q-1} S_\alpha(kf,q) \le \sum_{t=0}^{m-2} \varphi(q)\sqrt{p^{m-t}} = \varphi(q)\frac{p^{(m+1)/2}-p}{p^{1/2}-1},$$

and the result follows. $\square$

We now combine Proposition 10 and Beck's theorem [1, Theorem 3.1] to obtain an estimate for the number of lines spanned by C_i with $i = 1, 2, \ldots, p-1$, when $m \ge 3$. We first state Beck's theorem in its original version.

Theorem 12 (Beck)**.** *Let P be a set of n points in the plane. Then at least one of the following holds:*

(i) *There exists a line containing at least $n/100$ points of P.*
(ii) *For some positive constant c, there exist at least $c \cdot n^2$ distinct lines containing two or more points of P.*

Corollary 13. *If*

$$p^{m/2} + p^{(m-1)/2} - p^{1/2} - 1 < \frac{p^{m-1}}{100},$$

then the number of lines spanned by C_i with $i = 1, \ldots, p-1$, is at least $c \cdot p^{2(m-1)}$, where c is the constant in Beck's theorem.

Proof. We apply Beck's theorem with $P = C_i$. By Proposition 10 the first case of Beck's theorem does not hold. Hence C_i spans at least $c \cdot p^{2(m-1)}$ lines. □

2. Shparlinski's Question

One natural family of questions about finite point sets involves the various sets of distances they can determine. See for example [2] or [5]. In his survey paper [8] on the properties of $\mathcal{H}_{a,n}$, Shparlinski raises such a question.

Let $\mathcal{F}_{a,n}$ denote the set of Euclidean distances from the origin to points on $\overline{\mathcal{H}}_{a,n}$, that is,

$$\mathcal{F}_{a,n} = \{\sqrt{x^2+y^2} \,:\, (x,y) \in \overline{\mathcal{H}}_{a,n}\}.$$

In [8] Shparlinski presents a proof by the fourth author(AW) that

$$\#\mathcal{F}_{a,p} = \frac{p + (a/p)}{2}, \quad p > 2,$$

where p is prime, $\gcd(a,p) = 1$, and $(\cdot/p)$ is the Legendre symbol. It is natural to ask whether there is a similar formula for the cardinality $\#\mathcal{F}_{a,n}$ for general n. The points of $\overline{\mathcal{H}}_{a,n}$ are symmetric along the line $y = x$ which suggests that $\#\mathcal{F}_{a,n}$ is approximately $\varphi(n)/2$. The primary goal of this section is to adapt the proof in [8] to estimate the difference

$$\#\mathcal{F}_{a,n} - \frac{\varphi(n)}{2}$$

when $n = p^2$ with p an odd prime.

To simplify the notation we introduce a map $d_{a,n} : \mathbb{Z}_n^* \to \mathbb{Z}$ via

$$d_{a,n}(x) = (x \bmod n)^2 + \left(\left(a \cdot x^{-1}\right) \bmod n\right)^2.$$

Clearly $\#\mathrm{Image}(d_{a,n}) = \#\mathcal{F}_{a,n}$.

We now focus on estimating $\#\mathrm{Image}(d_{a,p^2})$.

We should remark that determining the cardinality of the set

$$\{(x^2+y^2) \mod n \,:\, (x,y) \in \overline{\mathcal{H}}_n\}$$

is easier and has been done in [7] using completely elementary methods, that is, algebraic manipulations in conjunction with the Chinese Remainder Theorem.

2.1. **Some notation.** We begin by defining a class of biquadratic polynomials and certain subsets of $\mathrm{Image}(d_{a,p^2})$ and $\mathbb{Z}_{p^2}^*$. Let $f_u(Z)$ denote the polynomial

$$f_u(Z) = Z^4 - uZ^2 + a^2.$$

Let $A \subseteq \mathrm{Image}(d_{a,p^2})$ be the set

$$A = \{u \in \mathrm{Image}(d_{a,p^2}) : f_u(Z), f_u'(Z) \text{ have no common root modulo } p\}$$

and let B be the complement of A in $\mathrm{Image}(d_{a,p^2})$.

Let B_1, B_2 be the following two subsets of $\mathrm{Image}(d_{a,p^2})$.

$$B_1 = \{d_{a,p^2}(l) : l \in \mathbb{Z}_{p^2}^*,\ \ l^2 - a \equiv 0 \pmod p\},$$

and

$$B_2 = \{d_{a,p^2}(l) : l \in \mathbb{Z}_{p^2}^*,\ \ l^2 + a \equiv 0 \pmod p\}.$$

Finally if a is a quadratic residue modulo p, then there is an integer $b, 0 < b < p$ such that $b^2 \equiv a \pmod p$. In this case we define the sets $C_1, C_2 \subseteq \mathbb{Z}_{p^2}^*$ via

$$C_1 = \{b + tp \,:\, 0 \le t \le p-1\},$$

$$C_2 = \{p - b + tp \,:\, 0 \le t \le p-1\}.$$

2.2. **Main result of Section 2 and proof.**

Proposition 14. *Let p be any prime. If $p \ge 3$, then*

$$\#\mathrm{Image}(d_{a,p^2}) = \frac{\varphi(p^2) + 1 + (a/p)}{2} - \#(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)).$$

Outline of proof of Proposition 11. The proof of the theorem is encapsulated in the following sequence of statements.

(a) We can associate each $u \in \mathrm{Image}(d_{a,p^2})$ with the congruence

$$f_u(Z) \equiv 0 \pmod{p^2}.$$

(b) Using properties of $f_u(Z)$ we show that for each $u \in A$, there are exactly two distinct elements $x_1, x_2 \in \mathbb{Z}_{p^2}^*$ such that

$$d_{a,p^2}(x_1) = d_{a,p^2}(x_2) = u.$$

(c) The cardinality of A is

$$\#A = \frac{\varphi(p^2) - \#d^{-1}_{a,p^2}(B)}{2}.$$

(d) The set B is the disjoint union of the sets B_1 and B_2. Consequently,

$$\#d^{-1}_{a,p^2}(B) = \#d^{-1}_{a,p^2}(B_1) + \#d^{-1}_{a,p^2}(B_2).$$

(e) If $B_2 \neq \emptyset$, then $\#d^{-1}_{a,p^2}(\{B_2\}) = 2p$ and $\#B_2 = p$.

(f) If $B_1 \neq \emptyset$, then $d^{-1}_{a,p^2}(\{B_1\}) = 2p$. Furthermore,

$$B_1 = d_{a,p^2}(C_1) \cup d_{a,p^2}(C_2)$$

with

$$\#d_{a,p^2}(C_i) = \frac{p-1}{2} + 1,$$

for $i = 1, 2$.

Proof of (a),(b) and (c). Let $u \in \mathrm{Image}(d_{a,p^2})$. Then $u = r_u^2 + (ar_u^{-1})^2$ for some $r_u \in \mathbb{Z}^*_{p^2}$ with $1 \leq r_u, ar_u^{-1} < p^2$. It immediately follows that r_u is a root of the congruence $f_u(Z) \equiv 0 \pmod p$.

We now turn to statements (b) and (c). Let $u \in A$ and let $r_u \in \mathbb{Z}^*_{p^2}$ such that $d_{a,p^2}(r_u) = u$. We claim that

$$d^{-1}_{a,p^2}(\{u\}) = \{r_u,\, ar_u^{-1}\}.$$

We first show $r_u \neq ar_u^{-1}$, by proving the contrapositive. Let $x = r_u \mod p$ and $y = ar_u^{-1} \mod p$. If $r_u = ar_u^{-1}$, then $x = y$, $x^2 \equiv a \pmod p$ and $u \equiv 2x^2 \pmod p$. It follows that $f_u(Z)$ factors as

$$f_u(Z) = Z^4 - uZ^2 + a^2 \equiv (Z-x)^2(Z+x)^2 \pmod p.$$

But this contradicts our assumption that $f_u(Z)$ and $f'_u(Z)$ do not have any roots in common modulo p. In a similar fashion we show that $ar_u^{-1} \neq p^2 - r_u$.

We now observe that $f_u(Z)$ has 4 four distinct roots modulo p: $x, y, p-x$ and $p-y$. Furthermore each root lifts to a *unique* root modulo p^2, that is, x lifts to r_u, y to ar_u^{-1}, $p-x$ to $(p^2 - r_u)$ and $p-y$ to $(p^2 - ar_u^{-1})$. Consequently $d^{-1}_{a,p^2}(\{u\}) \subseteq \{r_u,\, ar_u^{-1},\, p^2 - r_u,\, p^2 - ar_u^{-1}\}$. So to conclude the proof we need to prove that $d_{a,p^2}(r_u) \neq d_{a,p^2}(p^2 - r_u)$. If $d_{a,p^2}(r_u) = d_{a,p^2}(p^2 - r_u)$, then a simple calculation shows $ar_u^{-1} = (p^2 - r_u)$ which contradicts our earlier calculation that $ar_u^{-1} \neq p^2 - r_u$. □

Proof of (d). Let $d_{a,p^2}(r_u) = u$, where $u \in (\mathrm{Image}(d_{a,p^2}) \cap B)$ and let $x = r_u \mod p$. Since $u \in B$, x is a common root modulo p of the polynomials $f_u(Z) = Z^4 - uZ^2 + a^2$ and $f_u'(Z) = 4Z^3 - 2uZ$. It follows that $2x^2 = u \pmod p$ and

$$(a - x^2)(a + x^2) \equiv 0 \pmod p.$$

Therefore

$$x^2 \equiv a \pmod p \text{ and } u \equiv 2a \pmod p$$

or

$$x^2 \equiv -a \pmod p \text{ and } u \equiv -2a \pmod p.$$

In the first case $u \in B_1$, and in the second $u \in B_2$. Finally $B_1 \cap B_2 = \emptyset$ since $2a \not\equiv -2a \pmod p$. □

Proof of (e). If $B_2 \neq \emptyset$, then there exists an integer c with $1 \leq c \leq p-1$, such that $c^2 \equiv -a \pmod p$. It follows that $d_{a,p^2}^{-1}(B_2)$ is the disjoint union of the sets D_1, D_2 where

$$D_1 = \{c + tp \,:\, 0 \leq t \leq p-1\},$$

$$D_2 = \{p - c + tp \,:\, 0 \leq t \leq p-1\}.$$

Consequently, $\#d_{a,p^2}^{-1}(\{B_2\}) = 2p$.

Now there exists a unique integer l_p, $0 \leq l_p \leq p-1$, such that

$$c \cdot (p - c + l_p p) \equiv a \pmod{p^2}.$$

It follows that for $t = 0, 1, \ldots, p-1$,

$$\left(a \cdot (c+tp)^{-1}\right) \mod p^2 = \begin{cases} p - c + (l_p + t)p, & l_p + t < p \\ p - c + (l_p + t - p)p, & l_p + t \geq p. \end{cases}$$

From this we see that $x \in D_1$ if and only if $a \cdot x^{-1} \in D_2$, and we can conclude that the sets $d_{a,p^2}(D_1)$ and $d_{a,p^2}(D_2)$ are equal, and consequently $B_2 = d_{a,p^2}(D_1)$. So we are done if we can show that d_{a,p^2} is one-to-one on D_1. To do this we define the functions

$$f(t) = (c + tp)^2 + (p - c + (l_p + t)p)^2$$

and

$$g(t) = (c + tp)^2 + (p - c + (l_p + t - p)p)^2.$$

That is,

$$d_{a,p^2}(c+tp) = \begin{cases} f(t), & l_p + t < p, \\ g(t), & l_p + t \geq p. \end{cases}$$

A simple calculation shows that $f(t) = f(s)$ if and only if $s = t$. Similarly, $g(t) = g(s)$ if and only if $s = t$. Finally, if we try to solve the equation $f(t) = g(s)$, we get the contradiction that $2|p$. Thus we get that d_{a,p^2} is one-to-one on D_1. □

Proof of (f). If $B_1 \neq \emptyset$, then there exists an integer b with $1 \leq b \leq p-1$, such that $b^2 \equiv a \pmod p$. It follows that $d^{-1}_{a,p^2}(B_1)$ is the disjoint union of the sets C_1, C_2, where (we remind the reader)

$$C_1 = \{b + tp \,:\, 0 \leq t \leq p-1\}, \text{ and } C_2 = \{p - b + tp \,:\, 0 \leq t \leq p-1\}.$$

Consequently, $\#d^{-1}_{a,p^2}(\{B_1\}) = 2p$.

The remaining part of the proof is trickier than the case for B_2. This is because d_{a,p^2} is not one-to-one on C_1, nor are $d_{a,p^2}(C_1)$ and $d_{a,p^2}(C_2)$ equal as sets. We will prove that

$$\#d_{a,p^2}(C_1) = \#d_{a,p^2}(C_2) = \frac{p-1}{2} + 1.$$

Now there exists a unique integer j_p, $0 \leq j_p \leq p-1$, such that

$$b \cdot (b + j_p p) \equiv a \pmod{p^2}.$$

It follows that for $t = 0, 1, \ldots, p-1$,

$$\big(a \cdot (b+tp)^{-1}\big) \bmod p^2 = \begin{cases} b + (j_p - t)p, & t \leq j_p \\ b + (p + j_p - t)p, & t > j_p. \end{cases}$$

We now define the functions

$$f(t) = (b+tp)^2 + (b+(j_p-t)p)^2 \text{ and } g(t) = (b+tp)^2 + (b+(p+j_p-t)p)^2.$$

That is,

$$d_{a,p^2}(b+tp) = \begin{cases} f(t), & t \leq j_p \\ g(t), & t > j_p. \end{cases} \tag{3}$$

A simple calculation shows that $f(t) = f(s)$ if and only is $s = t$ or $s = j_p - t$. Similarly, $g(t) = g(s)$ if and only if $s = t$ or $s = p + j_p - t$. Finally if we try to solve the equation $f(t) = g(s)$ we get the contradiction that $2|p$. These observations combined with the observation that either

$(b + j_p p/2)$ or $(b + (j_p + p)p/2)$ is a solution of $x^2 \equiv a \pmod{p^2}$, give us the following:

(i) If j_p is even, then $\#f^{-1}(\{t\}) = 2$ for $t \le j_p, t \ne j_p/2$; $\#g^{-1}(\{t\}) = 2$ for $t > j_p$; and $\#f^{-1}(\{j_p/2\}) = 1$.

(ii) If j_p is odd, then $\#f^{-1}(\{t\}) = 2$ for $t \le j_p$; $\#g^{-1}(\{t\}) = 2$ for $t > j_p, t \ne (j_p + p)/2$; and $\#f^{-1}(\{(j_p + p)/2\}) = 1$.

We conclude that

$$\#d_{a,p^2}(C_1) = \frac{p-1}{2} + 1.$$

In a similar manner we show that $\#d_{a,p^2}(C_2) = (p-1)/2 + 1$.

In summary we see that if $(a/p) = 1$, then

$$\#B_1 = p + 1 - \#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right).$$

□

2.3. **Bounding** $\#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right)$**.** Thus the key difficulty to determining the cardinality $\#\mathrm{Image}(d_{a,p^2})$ is determining the cardinality of the intersection $d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)$. We now identify $C_1 \times C_2$ with the set $\{0, 1, \ldots, p-1\}^2$ via

$$(t, s) \mapsto (b + tp, p - b + sp)$$

and then define the map

$$l : \{0, 1, \ldots, p-1\}^2 \to \mathbb{Z}^2$$

via

$$l\left((t, s)\right) = (d_{a,p^2}(b + tp), d_{a,p^2}(p - b + sp)).$$

Clearly,

$$\#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right) = \#\left(l\left([0, p-1]^2\right) \cap \{(x, x) : x \in \mathbb{Z}\}\right).$$

In (3) we gave the form of $(a \cdot x^{-1}) \mod p^2$ when $x \in C_1$, and then obtained the distance function associated with C_1. Specifically

$$d_{a,p^2}(b + tp) = \begin{cases} f(t), & t \le j_p \\ g(t), & t > j_p \end{cases}$$

where

$$f(t) = (b+tp)^2 + (b+(j_p-t)p)^2, \text{ and } g(t) = (b+tp)^2 + (b+(p+j_p-t)p)^2.$$

We now state a similar form when $x \in C_2$. Put

$$k_p = \begin{cases} p - j_p - 2, & j_p \le p-2, \\ -1 & j_p = p-1. \end{cases}$$

Since $x \in C_2$, $x = p - b + sp$ for some s with $0 \le s \le p-1$. An immediate calculation gives us the following:

$$\left(a \cdot x^{-1}\right) \bmod p^2 = \begin{cases} p - b + (k_p - s)p, & s \le k_p, \\ p - b + (p + k_p - s)p, & s > k_p. \end{cases}$$

Put

$$F(s) = (p - b + sp)^2 + (p - b + (k_p - s)p)^2,$$

and

$$G(s) = (p - b + sp)^2 + (p - b + (p + k_p - s)p)^2.$$

Then we have

$$d_{a,p^2}(p - b + sp) = \begin{cases} F(s), & s \le k_p, \\ G(s), & s > k_p. \end{cases}$$

Proposition 15. *Let L_1, L_2 be the sets*

$$\begin{aligned} L_1 &= \{(t,s) \in [0, j_p/2] \times [k_p + 1, (p + k_p)/2] \cap \mathbb{Z}^2 : \\ &\qquad (s + t + 1 - p)(s - t + 1 + j_p - p) = 2b + j_p p - p^2\}, \end{aligned}$$

$$\begin{aligned} L_2 &= \{(t,s) \in [j_p + 1, (p + j_p)/2] \times [0, k_p/2] \cap \mathbb{Z}^2 : \\ &\qquad (s + t + 1 - p)(s - t + 1 + j_p) = 2b + j_p p\}. \end{aligned}$$

Then for $i = 1, 2$, if $L_i \neq \emptyset$, then l is injective on L_i. Furthermore,

$$l\left([0, p-1]^2\right) \cap \{(x,x) : x \in \mathbb{Z}\} = l(L_1) \cup l(L_2).$$

Proof. Let $(t,s) \in [0,p-1]^2 \cap \mathbb{Z}^2$ such that $d_{a,p^2}(b+tp) = d_{a,p^2}(p-b+sp)$. We consider two cases: (a) $j_p \le p-2$; (b) $j_p = p-1$.

Case (a) $j_p \le p-2$. In this case we are forced to consider four equations:

(i) $f(t) - F(s) = 0$: This has no solutions for integral s and t. (Otherwise we get the contradiction $2|p$.)

(ii) $g(t) - G(s) = 0$: Again this has no integer solutions for the same reason as above.

(iii) $f(t)-G(s)=0$: We have that $f(t)-G(s)$ equals the expression

$$2p^2(-2p^2+2sp+2pj_p+2p-sj_p-tj_p-1+t^2-j_p+2b-2s-s^2).$$

Consequently $f(t)-G(s)=0$ simplifies to

$$p^2-2sp-pj_p-2p+sj_p+tj_p+1-t^2+j_p+2s+s^2=2b+j_pp-p^2.$$

The LHS now factors to give

$$(s+t+1-p)(s-t+1+j_p-p)=2b+j_pp-p^2. \tag{4}$$

(iv) $g(t)-F(s)=0$: We have that $g(t)-F(s)$ equals the expression

$$2p^2(2pj_p-tp+sp+p-sj_p-tj_p-1+t^2-j_p+2b-2s-s^2).$$

Consequently $g(t)-F(s)=0$ simplifies to

$$-pj_p+tp-sp-p+sj_p+tj_p+1-t^2+j_p+2s+s^2=2b+j_pp.$$

The LHS now factors to give

$$(s+t+1-p)(s-t+1+j_p)=2b+j_pp. \tag{5}$$

Case (b) $j_p=p-1$. In this case we consider the equation $f(t)-G(s)=0$. We have that

$$f(t)-G(s)=2p^2(sp-tp-p+t^2+t-s^2+2b-s).$$

Consequently $f(t)-G(s)=0$ simplifies to

$$(-sp+tp-t^2-t+s^2+s)=2b-p.$$

The LHS factors to give

$$(s-t)(s+t+1-p)=2b-p,$$

which we note is the same as (4) with $j_p=p-1$.

Thus we have proved that (t,s) satisfies either (4) or (5). Furthermore, it is easy to check that any point $(t,s)\in[0,p-1]^2\cap\mathbb{Z}^2$ satisfying either (4) or (5) must give that $d_{a,p^2}(b+tp)=d_{a,p^2}(p-b+sp)$. Thus to complete the proof we need to restrict ourselves to sets where l is injective.

We now note the following:

(I) $f(t_2)=f(t_1)$ if and only if $t_2=j_p-t_1$.
(II) $G(s_2)=G(s_1)$ if and only if $s_2=p-k_p-s_1$.
(III) $g(t_2)=g(t_1)$ if and only if $t_2=p+j_p-t_1$.
(IV) $F(s_2)=F(s_1)$ if and only if $s_2=k_p-s_1$.

The condition for equation (4) arose when we considered the equation $f(t) = G(s)$. If we restrict ourselves to values of t and s satisfying this equation to the intervals $0 \le t \le j_p/2$, $k_p + 1 \le s \le (p + k_p)/2$, we get that l is injective. The condition for equation (5) arose when we considered the equation $g(t) = F(s)$. If we restrict ourselves to values of t and s satisfying this equation to the intervals $j_p+1 \le t \le (p+j_p)/2$, $0 \le s \le k_p/2$, we get that l is injective. We conclude that

$$l\left([0, p-1]^2\right) \cap \{(x, x) \,:\, x \in \mathbb{Z}\} = l(L_1) \cup l(L_2)$$

and consequently

$$\#\left(l\left([0, p-1]^2\right) \cap \{(x, x) \,:\, x \in \mathbb{Z}\}\right) = \#l(L_1) + \#l(L_2).$$

□

The interesting case of the previous proposition is the case for $j_p = 0$. By setting $m = (s+t+1-p)$ and $n = (s-t+1)$, and then manipulating various inequalities we obtain the following corollary.

Corollary 16. *Let $j_p = 0$ and let S denote the set of lattice points $(m, n) \in \mathbb{Z}^2$ with $mn = 2b$ satisfying the additional conditions:*

$$-p + 2 \le m < 0, \; -p/2 + 1 \le n < 0, \; m \not\equiv n \pmod 2, \; m \le n.$$

Then

$$\#S = \#l(L_2) = \#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right).$$

We now have the following two corollaries.

Corollary 17. *For $p \ge 5$, $\#\left(d_{1,p^2}(C_1) \cap d_{1,p^2}(C_2)\right) = 1$; consequently $\#\mathrm{Image}(d_{1,p^2}) = \varphi(p^2)/2$.*

Proof. Since $a = 1$, we have $j_p = 0$. Invoking Corollary 16 we get that $S = \{(-2, -1)\}$. □

Corollary 18. *Let*

$$M_{p^2} = \max\left(\left\{\, \varphi(p^2)/2 - \#\mathrm{Image}(d_{a,p^2}) \,:\, 1 \le a < p^2, \; \gcd(a, p) = 1\right\}\right).$$

Then

$$\lim_{p\to\infty} (M_{p^2}) = \infty.$$

Proof. Let $a = p_1^2 p_2^2 \dots p_n^2$, where p_i is the i-th odd prime, and let p be a prime larger than a. Now $b = p_1 p_2 \dots p_n$ and $j_p = 0$, and therefore we can apply Corollary 16. The cardinality of S (the set defined in Corollary 16) equals 2^n. We now let p and n go to infinity to obtain our conclusion. □

2.4. **The case $n = p^m$, $m \geq 3$.** The reader should note for p^m with $m \geq 3$, the proofs of statements (a),(b),(c) and (d) extend automatically. The higher power case starts to diverge from our earlier work when we start to consider the counterparts of the sets B_1 and B_2, which we denote as B_{1,p^m}, B_{2,p^m}, that is,

$$B_{1,p^m} = \{d_{a,p^m}(l) : l \in \mathbb{Z}_{p^m}^*, \;\; l^2 - a \equiv 0 \pmod{p}\},$$

and

$$B_{2,p^m} = \{d_{a,p^m}(l) : l \in \mathbb{Z}_{p^m}^*, \;\; l^2 + a \equiv 0 \pmod{p}\}.$$

The proofs that $\#d_{a,p^2}^{-1}(\{B_1\}) = 2p$ when $B_1 \neq \emptyset$, and $\#d_{a,p^2}^{-1}(\{B_2\}) = 2p$ when $B_2 \neq \emptyset$, extend to the general case. So we have the following.

Proposition 19. *For $i = 1, 2$, if $B_{i,p^m} \neq \emptyset$, then*

$$\#d_{a,p^m}^{-1}(B_{i,p^m}) = 2p^{m-1}.$$

Consequently,

$$\begin{aligned} \#\mathrm{Image}(d_{a,p^m}) - \frac{\varphi(p^m)}{2} &= \left(\#B_{1,p^m} - \frac{(1 + (a/p))p^{m-1}}{4}\right) \\ &+ \left(\#B_{2,p^m} - \frac{(1 + (-a/p))p^{m-1}}{4}\right). \end{aligned}$$

In particular when $(a/p) = (-a/p) = -1$, and consequently $B_{1,p^m} = B_{2,p^m} = \emptyset$, then

$$\#\mathrm{Image}(d_{a,p^m}) = \frac{\varphi(p^m)}{2}. \tag{6}$$

At this juncture our results for B_{1,p^m} or B_{2,p^m} start to diverge from our results for B_1 and B_2. They are weaker and consequently, we end up deriving upper and lower bounds for the difference

$$\#\mathrm{Image}(d_{a,p^m}) - \frac{\varphi(p^m)}{2}.$$

Proposition 20. *We have the following:*

(i) $\#B_{1,p^m} \leq p^{m-1} + 1.$

(ii) $\#B_{2,p^m} \leq p^{m-1}$.

(iii) *Let $\mathcal{C}$ denote a circle with center the origin. Then*

$$\#\left(d_{a,p^m}^{-1}(B_{i,p^m}) \cap \mathcal{C}\right) < p^{m/2} + p^{(m-1)/2} - p^{1/2}.$$

(iv) *For $i = 1, 2$, if $B_{i,p^m} \neq \emptyset$, then*

$$\#B_{i,p^m} \geq \frac{2p^{m-1}}{p^{m/2} + p^{(m-1)/2} - p^{1/2}}.$$

(v) *If $B_{1,p^m} \cup B_{2,p^m} \neq \emptyset$, then*

$$kp^{m-1}\left(\frac{1}{p^{m/2} + p^{(m-1)/2} - p^{1/2}} - \frac{1}{2}\right) \leq \#\mathrm{Image}(d_{a,p^m}) - \frac{\varphi(p^m)}{2} \leq 1,$$

where

$$k = \begin{cases} 2, & (a/p) \cdot (-a/p) = -1 \\ 4, & (a/p) = (-a/p) = 1. \end{cases}$$

Remarks. We simply make some remarks as the proofs are similar to what has been done earlier. To prove (i), we take an arbitrary $l \in d_{a,p^m}^{-1}(B_{1,p^m})$ and then set $l' = a \cdot l^{-1} \mod p^m$. Since, $d_{a,p^m}(l) = d_{a,p^m}(l')$,

$$\#d_{a,p^m}^{-1}(\{d_{a,p^m}(l)\}) \geq 2,$$

except possibly when $l = a{\cdot}l^{-1} \mod p^m$, that is, l is a solution of $x^2 \equiv a \pmod{p^m}$. These observations combined with our earlier observation that if $B_{1,p^m} \neq \emptyset$, then $\#d_{a,p^m}^{-1}(B_{1,p^m}) = 2p^{m-1}$ gives (i). Inequality (ii) is proved in a similar way. The proof of inequality (iii) is similar to the proof of Proposition 10. □

2.5. **Some computed values of $\#\mathcal{F}_{a,p^m}$.** We conclude with the following tables of some small values of $\#\mathcal{F}_{a,p^m}$ computed directly. We point out that the lines corresponding to $\#\mathcal{F}_{2,5^m}$ and $\#\mathcal{F}_{3,5^m}$ are redundant. This is because $(2/5) = (3/5) = -1$ and so we can simply invoke (6).

m	1	2	3	4	5	6	7	8	9	10
$\phi(3^m)/2$	1	3	9	27	81	243	729	2187	6561	19683
$\#\mathcal{F}_{1,3^m}$	2	4	10	26	81	243	728	2185	6560	19682
$\#\mathcal{F}_{2,3^m}$	1	3	9	27	81	243	729	2187	6561	19683
$\#\mathcal{F}_{4,3^m}$	2	4	10	27	81	243	729	2185	6559	19681

m	1	2	3	4	5	6	7
$\phi(5^m)/2$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{1,5^m}$	3	10	51	249	1251	6248	31250
$\#\mathcal{F}_{2,5^m}$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{3,5^m}$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{4,5^m}$	3	11	51	249	1251	6249	31248

m	1	2	3	4	5	6	7
$\phi(7^m)/2$	3	21	147	1029	7203	50421	352947
$\#\mathcal{F}_{1,7^m}$	4	21	148	1027	7203	50421	352946
$\#\mathcal{F}_{2,7^m}$	4	22	147	1029	7204	50420	352943
$\#\mathcal{F}_{3,7^m}$	3	21	147	1029	7203	50421	352947
$\#\mathcal{F}_{4,7^m}$	4	21	148	1027	7204	50421	352946

References

[1] J. Beck, On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry, *Combinatorica*, **3**(1983), no. 3-4, 281–297.

[2] P. Brass, W. Moser, and J. Pach, *Research Problems in Discrete Geometry,* Springer (2005).

[3] T. Cochrane and Z. Zheng, Pure and mixed exponential sums, *Acta Arith.*, **91** (1999), no. 3, 249–278.

[4] J. Csima and E. T. Sawyer, There exist $6n/13$ ordinary points, *Discrete Comput Geom.* **9** (1993), no.2, 187–202.

[5] J. Garibaldi, A. Iosevich, and S. Senger, *The Erdős Distance problem,* AMS Student Mathematical Library Volume 56 (2011).

[6] B. Green and T. Tao, On sets defining few ordinary lines, preprint available at http://arxiv.org/abs/1208.4714, (2013), 1–72.

[7] S. Hanrahan and M. R. Khan, The cardinality of the value sets of $\left(x^2 + x^{-2}\right)$ mod n and $\left(x^2 + y^2\right)$ mod n, *Involve* 3:2 (2010), 171–182.

[8] I. E. Shparlinski, Modular hyperbolas, *Japan J. Math.*, 7:2 (2012), 235–294. (Also available at http://arxiv.org/abs/1103.2879)

MRK: Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, CT 06226, USA
E-mail address: khanm@easternct.edu

RM: Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, CT 06226
E-mail address: magnerri@my.easternct.edu

SS: Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
E-mail address: senger@math.udel.edu

AW: Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Str. 69, A-4040 Linz,Austria
E-mail address: arne.winterhof@oeaw.ac.at